APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/928,026	08/10/2001	Lauri Piikivi	617-010487-US(PAR)	5196

2512   7590   08/18/2009

Perman & Green, LLP
99 Hawley Lane
Stratford, CT 06614

EXAMINER
TESLOVICH, TAMARA

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
08/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>26 May 2009</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-15</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-15</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

    1.☐ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

This Office Action is in response to Applicant's Remarks and Amendments filed

May 26, 2009.

Claims 1-4, 6, 7, 9, 14, and 15 have been amended.

Claim 16 is cancelled.

Claims 1-15 are pending and herein considered.

Response to Arguments

Applicant's arguments filed May 26, 2009 have been fully considered but they are

not persuasive.

In response to Applicant's remarks concerning Dominguez' alleged failure to

teach or suggest "a selector configured to be connected to and to receive a control

message signal from said second party, said signal including a plurality of

communication security protocols for protecting information transmitted over the

communication link" and "the selector further configured in response to receiving the

control message signal, to select one of the plurality of communication security

protocols so that information subsequently transmitted over the communication link

between the devices and the second party is protected using the selected

communication security protocol" as taught in claim 1, the Examiner respectfully

disagrees. Applicant attempts to distinguish his communication security protocol from

the authentication security protocols in Dominguez but fails to account for the ample

teachings within Dominguez regarding the use of secure communication protocols in addition to authentication protocols. The Examiner would like to draw attention to paragraphs 57, 67, 72-73, 82, and 84-88 wherein Dominguez discloses the use of secure communication protocols including but not limited to SSL. While each of these paragraphs provides for the use of secure communication protocols, paragraphs 84-88 in particular provide for the use of multiple channels which utilize differing secure communication protocols and may be selected in response to a particular need in order that information subsequently transmitted over the communication link between the device and the second party may be protected using the selected communication protocol. It is in view of the above mentioned paragraphs in view of the Dominguez reference in its entirety, particularly its repeated disclosure of the use of a variety of secure communication protocols, that the Examiner maintains her rejection of the claims as anticipated by the Dominguez reference.

In response to Applicant's remarks concerning Dominguez' alleged failure to teach or suggest "a selector configured for selecting one of a plurality of communication security protocols for protecting information transmitted over the communication link, and being connected to communicate said selection to said second party" as taught in claim 14, the Examiner respectfully disagrees. Applicant's remarks are premised upon those given in response to the Examiner's rejection of similar language in claim 1, and are unpersuasive for the same reasons as presented above with regards to claim 1.

In response to Applicant's next set of remarks concerning Dominguez' alleged failure to teach or suggest "a calculator for generating a cryptogram for use with the

selected communication security protocol, and for transmittal from said device so that information transferred subsequently between the device and the second party is protected using the selected communication security protocol" as claimed in claim 14, the Examiner respectfully disagrees. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Furthermore, Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections. The citation of a particular claim limitation in and of itself is insufficient to show that a reference fails to teach such a limitation. Applicant has failed to provide the Examiner with any explanation as to why the prior art relied upon is insufficient to teach such a limitation.

Applicant's next set of arguments concerning claim 15 fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Furthermore, Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections. Applicant's citation of the

language of claim 15 following by a general statement regarding his inability to find anything in the reference that teaches such language is insufficient in view of the Examiner's outstanding rejection and in view of the existence of similar language in independent claims 1 and 14, each of which are discussed above.

In response to the Applicant's arguments concerning Williams' alleged failure to teach or suggest "a selector configured to be connected to and to receive a control message signal from said second party, said signal including a plurality of communication security protocols for protecting information transmitted over the communication link" and "the selector further configured in response to receiving the control message signal, to select one of the plurality of communication security protocols so that information subsequently transmitted over the communication link between the devices and the second party is protected using the selected communication security protocol" as taught in claim 1, the Examiner respectfully disagrees. The Examiner would like to draw attention to column 15, lines 1-21 wherein Williams clearly discloses support for cryptographic functionality including encryption, signatures, and key generation. Williams goes on to suggest that choice of key exchange algorithm, symmetric encryption algorithm, and signature algorithms should all be configurable and that the particular system components depend on the implementation selected for a particular customer. Williams goes on in column 17 lines 15-16 as well as column 18 lines 1-11 to discuss the importance of accepting and making payments in a secure and reliable manner, including the selection of security protocols relied upon to transfer that information. This ability to configure particular

communication security protocols based upon the desires and needs of a particular user

and their system, anticipates Applicant's selection configured to select a particular

communication security protocol and use that protocol for future communications as

claimed in claim 1.

In view of the arguments previous, Examiner respectfully disagrees with the

Applicant's argument that Dominguez fails to disclose claims 1-15 in their entirety, and

maintains the previously presented 35 U.S.C. 102(e) rejections repeated below in a

form to reflect Applicant's amendments. The Examiner also respectfully disagrees with

the Applicant's argument that Williams fails to disclose claims 1-2, 5, 8-10, 11 and 13 in

their entirety, and maintains the previously presented 35 U.S.C. 102(e) rejections

repeated below in a form to reflect Applicant's amendments.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form

the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

**Claims 1-15 are rejected under 35 U.S.C. 102(e) as being anticipated by
Dominguez et al. (US Patent Application Publication 2002/0194138).**

As per **Claim 1**, Dominguez teaches a device comprising a connecting

mechanism for establishing a communication link with a second party and a selector

configured to be connected to and to receive a control message signal from said second

party, said signal including a plurality of communication security protocols for protecting

information transmitted over the communication link and the selector further configured

in response to receiving the control message signal, to select one of the plurality of

communication security protocols so that information subsequently transmitted over the

communication link between the devices and the second party is protected using the

selected communication security protocol (pars 69-70, 76, 82).

As per **Claim 2**, Dominguez teaches selection means further comprises an

analyzer for analyzing the data contained in said control message signal and in

response thereto for selecting the communication security protocol (pars 76, 82).

As per **Claim 3**, Dominguez teaches a calculator for generating a cryptogram

from data held in at least one data field of the control message signal (pars 68-69, 219).

As per **Claim 4**, Dominguez teaches a cryptogram transmitter provided to

transmit the cryptogram from the mobile station to initiate secure transfer of information

from the device (pars 68-69, 219).

As per **Claim 5**, Dominguez teaches an application to provide a start payment

signal from the device to the second party which thereby initiates the control message

signal from the second party (par 33).

As per **Claim 6**, Dominguez teaches a mechanism for communicating, with a modified wallet server which is adapted to receive a cryptogram generated by the device and thereafter to communicate with a payment gateway via the second party (par 45). Note: The Examiner has relied on the above-cited paragraph to demonstrate Dominguez's use of secure wallets within his invention and the modes of communication associated with them.

As per **Claim 7**, Dominguez teaches means for communicating, with the second party directly utilizing a cryptogram generated via the device for use with the selected communication security protocol (par 68-69, 219).

As per **Claim 8**, Dominguez teaches 1 wherein the control message signal includes a series of data fields each containing data indicating a predetermined parameter for the information transfer (pars 72-76).

As per **Claim 9**, Dominguez teaches wherein the control signal includes a data field which indicates whether the device can communicate directly with the second party or with the second party via a modified wallet (par 45).

As per **Claim 10**, Dominguez teaches internet browsing circuitry which enables a user of the device to access and browse the internet via the device (pars 14, 33, 35, 36, 38).

As per **Claim 11**, Dominguez teaches connecting mechanism enables a connection to be established between said device and a second party via the Internet (pars 14, 33, 35, 36, 38).

As per **Claim 12**, Dominguez teaches wherein said device comprises a mobile station (par 38).

As per **Claim 13**, Dominguez teaches wherein said second party comprises a merchant server associated with a merchant offering an item to be purchased (par 3).

As per **Claim 14**, Dominguez teaches a device comprising a connecting mechanism for establishing a communication link with a second party, a selector configured for selecting one of a plurality of communication security protocols for protecting information transmitted over the communication link, and being connected to communicate said selection to said second party (pars 69-70, 76, 82), a calculator for generating a cryptogram for use with the selected communication security protocol, and for transmittal from said device so that information transferred subsequently between the device and the second party is protected using the selected communication security protocol, so that information transferred subsequently between the device and second party is protected using the selected security protocol (pars 68-70, 76, 82, 219).

As per **Claim 15**, Dominguez teaches a device comprising a connecting mechanism for establishing a communication link with a second party,

a receiver for receiving a control message signal from the second party specifying a communication security protocol for protecting transmitted information;

a calculator for generating a cryptogram for use with the selected communication security protocol and for transmittal from said devices to a third party, the third party configured in response to receiving the cryptogram to initiate communication with the second party using the communication security protocol so that information transferred

subsequently between the third party and the second party is protected using the

security protocol (pars 45, 69-70, 76, 82). Note: The Examiner has relied on the above-

cited paragraphs to demonstrate Dominguez's use of secure wallets within his invention

and the modes of communication associated with them.

Claims 1-2, 5, 8-10, 11, and 13 are rejected under 35 U.S.C. 102(e) as being

anticipated by Williams et al. (US Patent No. 5,963,924).

As per **Claim 1**, Williams teaches a device comprising a connecting mechanism

for establishing a communication link with a second party and a selector configured to

be connected to and to receive a control message signal from said second party, said

signal including a plurality of communication security protocols for protecting information

transmitted over the communication link and the selector further configured in response

to receiving the control message signal, to select one of the plurality of communication

security protocols so that information subsequently transmitted over the communication

link between the devices and the second party is protected using the selected

communication security protocol (col.15, lines 1-21; col.17 lines 15-16; col.18 lines 1-

11).

As per **Claim 2**, Williams teaches an analyzer for analyzing the data contained in

said control message signal and in response thereto for selecting the communication

security protocol (col.13 lines 51-54; col.15 lines 54-56; col.16 lines 53-56).

As per **Claim 5**, Williams teaches an application to provide a start payment signal from the device to the second party which thereby initiates the control message signal from the second party (col.15 lines 53-55).

As per **Claim 8**, Williams teaches wherein the control message signal includes a series of data fields each containing data indicating a predetermined parameter for the information transfer (col.15 lines 53-55).

As per **Claim 9**, Williams teaches wherein the control signal includes a data field which indicates whether the device can communicate directly with the second party or with the second party via a modified wallet (col.14 lines 8-24).

As per **Claim 10**, Williams teaches internet browsing circuitry which enables a user of the device to access and browse the internet via the device (abstract, col.10 line 38 thru col.11 line 12; col.9 lines 27-67).

As per **Claim 11**, Williams teaches wherein said connecting mechanism enables a connection to be established between said device and a second party via the Internet (abstract, col.10 line 38 thru col.11 line 12; col.9 lines 27-67).

As per **Claim 13**, Williams teaches wherein said second party comprises a merchant server associated with a merchant offering an item to be purchased (abstract, col.10 line 38 thru col.11 line 12).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Tamara Teslovich whose telephone number is (571)

272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/

Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437